Office of Information Security Newsletter

April 2006
Volume 1 Issue 3

INSIDE THIS ISSUE

1 Social Engineering

2 Network Vulnerability Assessments

SECURITY AWARENESS TRAINING UPDATE

The **Nevada Commission of Mineral Resources** was the first stand-alone Agency to complete the Security Training. Congratulations!

To date our awareness training website has been visited 13,024 times.

SOCIAL ENGINEERING

What is Social Engineering?

It is basically the art of getting people to comply with your wishes. It is not mind control, it will not allow you to get people to perform some crazy tasks that are outside the realm of their normal behavior and it is far from foolproof.

Social engineering can involve a lot of prep work such as information gathering and chatting about seemingly innocent topics, such was the case in the following experience. “Looks like the data pirates have the upper hand as they've begun stooping to tactics like pretending to be handicapped customers and service provider employees, with the aim of wrestling your info from gullible call-center workers. According to a suit filed by Verizon, data brokers have made thousands of calls to the company's customer service center, often posing as employees from a nonexistent "special needs" division of Verizon, which, according to the callers, was designed to help speech-impaired customers.” Source Engadget.com January 18, 2006

The most important part of the social engineering set-up is the human element, which means that this security weakness (people) is universal. Any type of information that can be gained may be used to take the attacker one step closer to their target.

The following are suggestions to help protect your Agency:

- Put procedures in place that out line steps to take if callers request information.
- Train all employees and let them know they have a part in protecting the State.
- Let employees know they do not have to be pushed around, if someone tries to threaten them or confuse them, it should raise a red flag.
- Always stay alert when dealing with callers.

NETWORK VULNERABILITY ASSESSMENTS

The Office of Information Security (OIS) - assessment unit performs regular security assessments across the State of Nevada. OIS will also perform information security vulnerability assessments on a request basis to assist agencies in improving their security posture.

Vulnerability Assessments can provide agencies with a wealth of valuable information about the level of exposure to threats.

The internal network is most often overlooked in information security management. Many organizations have strong external defenses, but almost nonexistent internal defenses. The State's SilverNet firewall can only protect internet related communication. An assessment will provide agencies with data on what an informed hacker or disgruntled employee might be able to accomplish from within.

Vulnerability assessments are an essential component in an effective information security program. Vulnerability assessments can provide agencies with a wealth of valuable information about the level of exposure to threats. Continuously conducting assessments of critical, high-risk information assets helps to proactively fortify the State's environment against emerging threats.

In the fast moving IT world where new vulnerabilities are found daily a regular Network Vulnerability Assessment schedule is an invaluable network security tool. A Network Vulnerability Assessment can alert agencies to potential vulnerabilities in their network **before** a hacker alerts the State to those vulnerabilities the hard way.

A full Network Vulnerability Assessment will analyze every IP address, computer, server, desktop and network device on a network and identify any potential holes a hacker could exploit. A more typical Network Vulnerability Assessment is targeted as a subset of these, usually supporting a critical application or highly sensitive data. For each vulnerability found, OIS will provide a recommended fix or workaround to mitigate the risk. Assessments provide agencies with the knowledge and means to be pro-active in securing their network, systems and more importantly, data.

In order to prevent problems before they start, OIS recommends a regular Network Vulnerability Assessment of critical systems. At the very least, organizations should undergo a Network Vulnerability Assessment once a year in addition to any time there is a suspicion of/or an actual compromise. A vulnerability Assessment should be done when a new system is installed, rebuilt or is changed to confirm the intended security posture of the system. It also helps prove "due diligence" in performing basic system patches and fixing the well-known problems in case of a security incident.

When Was Your Last Network Vulnerability Assessment?

Defending Nevada's Technology

State of Nevada
Office of Information Security - DoIT
1340 S. Curry Street
Carson City, NV 89703
Phone (775) 684-5800
Fax (775) 687-1155
Email: infosec@state.nv.us
Website: http://infosec.nv.gov